Federal Cybersecurity Research and Development Program: Strategic Plan

Federal Cybersecurity Research and Development Program: Strategic Plan

Dr. Douglas Maughan
Division Director, Cyber Security Division, Science & Technology Directorate, Department of Homeland Security (DHS S&T)

Dr. Carl Landwehr
Program Director, Trustworthy Computing Program, National Science Foundation (NSF)

Brad Martin
S&T Lead for Cyber
Office of the Director of National Intelligence/ National Security Agency (ODNI/NSA)

Presented by Federal NITRD Program

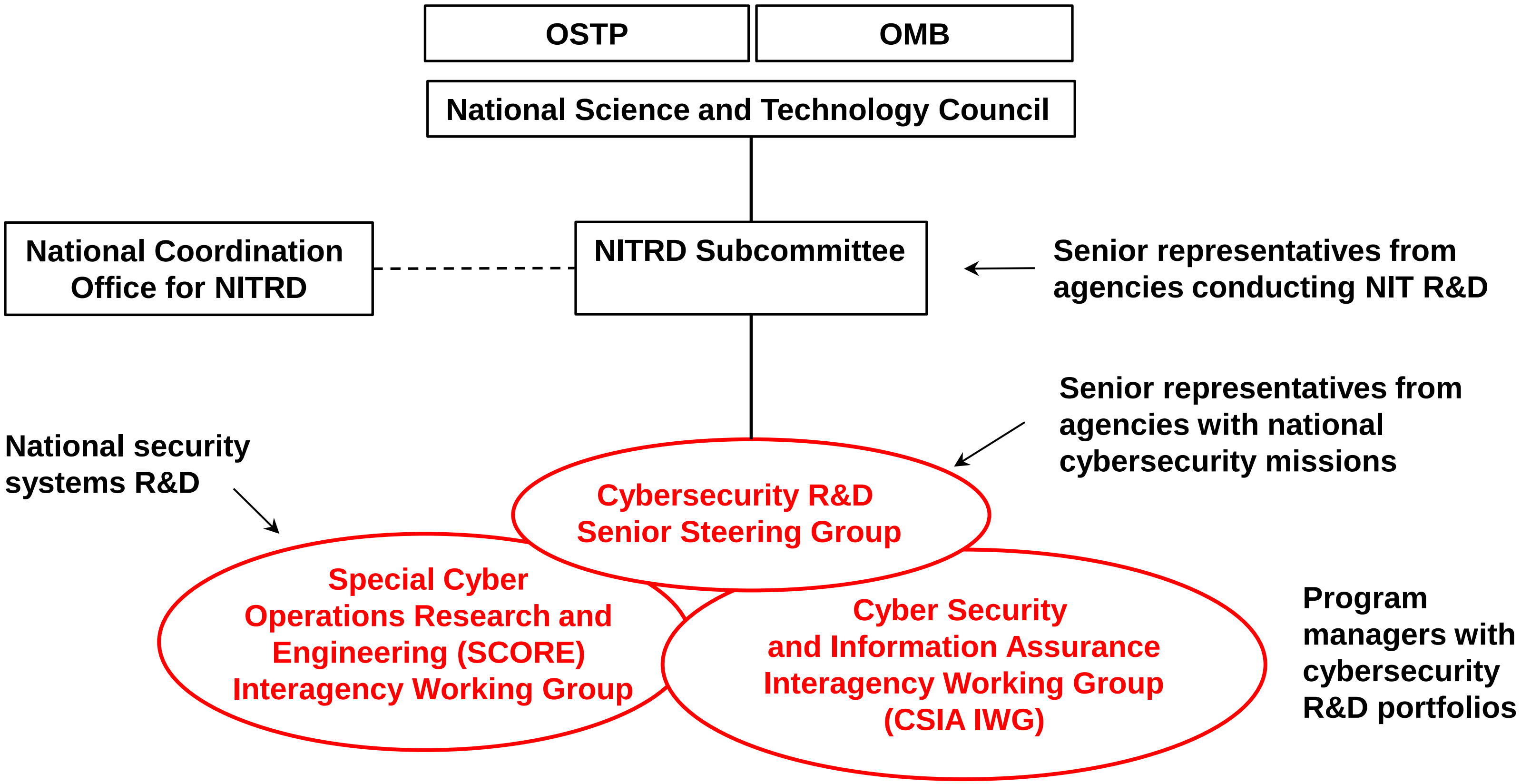
May 25, 2011

Claremont Hotel
41 Tunnel Road
Berkeley, California

NITRD Program

- Purpose
  - The primary mechanism by which the U.S. Government coordinates its unclassified Networking and IT R&D (NITRD) investments
  - Support NIT-related policy making in the White House Office of Science and Technology Policy (OSTP)
- Scope
  - Approximately $4B/year across 14 agencies, seven program areas
  - Cyber Security and Information Assurance (CSIA)
  - Human Computer Interaction and Information Management (HCI&IM)
  - High Confidence Software and Systems (HCSS)
  - High End Computing (HEC)
  - Large Scale Networking (LSN)
  - Software Design and Productivity (SDP)
  - Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)

NITRD Structure for Cybersecurity R&D Coordination



Federal Cybersecurity R&D Strategic Thrusts

- Research Themes
- Science of Cyber Security
- Transition to Practice
- Support for National Priorities

R&D Coordination Through Themes

- Theme $\neq$ Hard Problem
- To compel a new way of operating / doing business
- To attack underlying causes to bring about changes
- To provide shared vision of desired end state
- Established through robust community discussion of what matters
- Recognizes that independent thinking is vital to good research

Research Themes

Initial Themes (2010)

- Tailored Trustworthy Spaces
  – Supporting context specific trust decisions
- Moving Target
  – Providing resilience through agility
- Cyber Economic Incentives
  – Providing incentives to good security

New Theme (2011)

- Designed-in Security
  – Developing and evolving secure software systems

Annually re-examine themes, enrich with new concept, provide further definition or decomposition

Tailored Trustworthy Spaces

In the physical world, we operate in many spaces with many characteristics

- Home, school, workplace, shopping mall, doctor's office, bank, theatre
- Different behaviors and controls are appropriate in different spaces

Yet we tend to treat the cyber world as a homogenous, undifferentiated space

⇨ TTS: a flexible, distributed trust environment that can support functional, policy, and trustworthiness requirements arising from a wide spectrum of activities in the face of an evolving range of threats

TTS Paradigm

- Users can select/create different environments for different activities satisfying variety of operating capabilities
  - Confidentiality, anonymity, data and system integrity, provenance, availability, performance
- Users can negotiate with others to create new environments with mutually agreed characteristics and lifetimes
- Must be able to base trust decisions on verifiable assertions

Moving Target

- Controlled change across multiple system dimensions to:
  - Increase uncertainty and apparent complexity for attackers, reduce their windows of opportunity, and increase their costs in time and effort
  - Increase resiliency and fault tolerance within a system

Moving Target Paradigm

- All systems are compromised; perfect security is unattainable
- Objective is to continue safe operation in a compromised environment, to have systems that are defensible, rather than perfectly secure
- Shift burden of processing onto attackers

Cyber Economics & Incentives

- A focus on what impacts cyber economics and what incentives can be provided to enable ubiquitous security:
  - New theories and models of investments, markets, and the social dimensions of cyber economics
  - Data, data, and more data with measurement and analysis based on that data
  - Improved SW development models and support for “personal data ownership”

CEI Paradigm

- Promotion of science-based understanding of markets, decision-making and investment motivation
  - Security deployment decisions based on knowledge, metrics, and proper motivations
  - Promote the role of economics as part of that understanding
- Creation of environments where deployment of security technology is balanced
  - Incentives to engage in socially responsible behavior
  - Deterrence for those who participate in criminal and malicious behavior

Brad Martin

ODNI/NSA

Designed-in Security

- New research theme
- Designing and developing SW systems that are resistant to attacks
- Generating assurance artifacts to attest to the system’s capabilities to withstand attacks

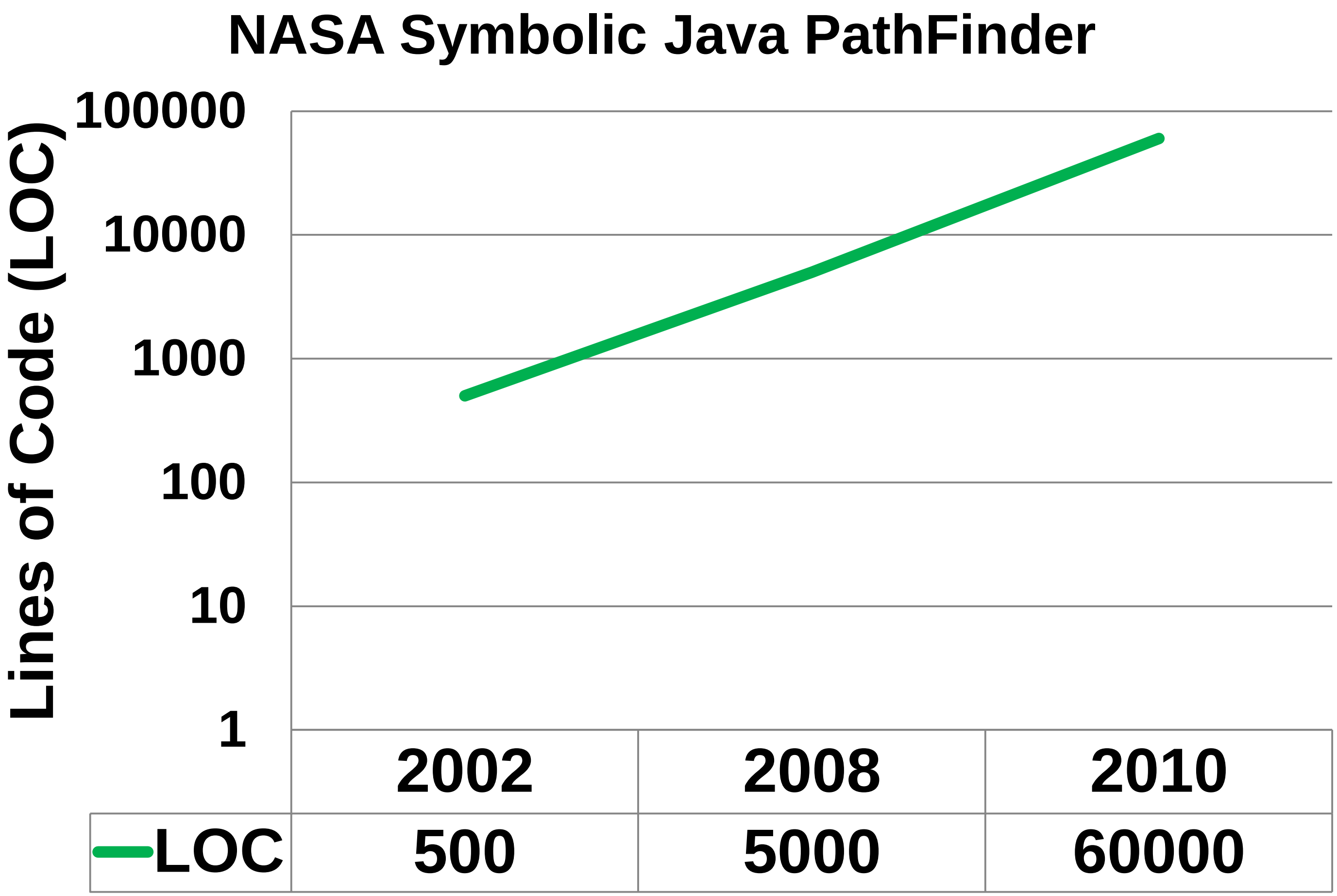
Designed-in Security Paradigm

- Require verifiable assurance about system's attack-resistance to be natively part of the SW design, development, and evolution lifecycle
- Enable reasoning about a diversity of quality attributes (security, safety, reliability, etc.) and the required assurance evidence
- Stimulate further developments in methods and tools for detecting flaws in SW

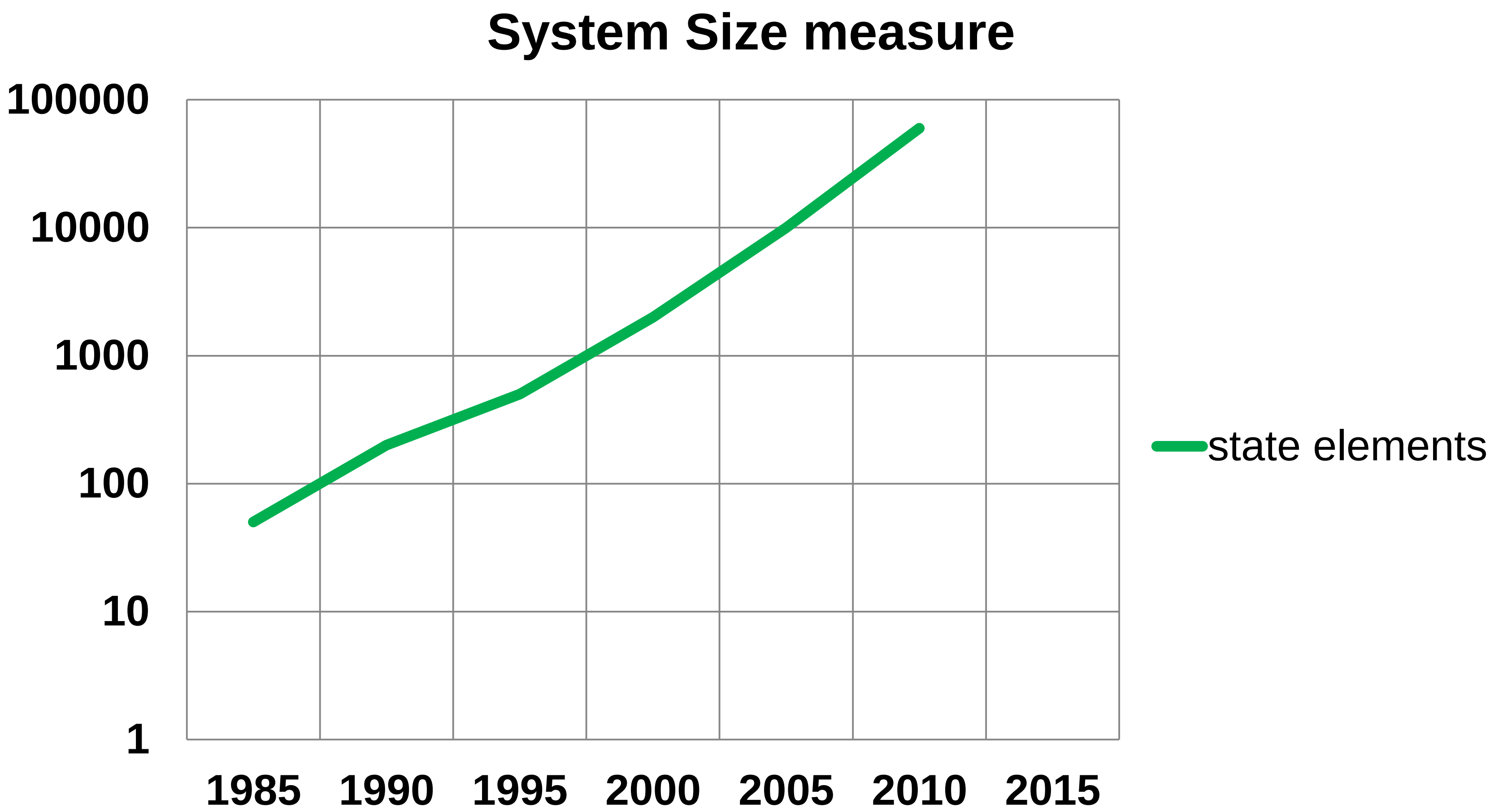
Software System Development Today: Assertions without Proof

- Programmers are expensive
- Tools are used to economize programmer productivity
- Programs grow in pieces from many sources
- Assuring security properties of a system of programs is very difficult
- Most systems of programs are low assurance
- High assurance programs are changed reluctantly

Progress: Dynamic Analysis

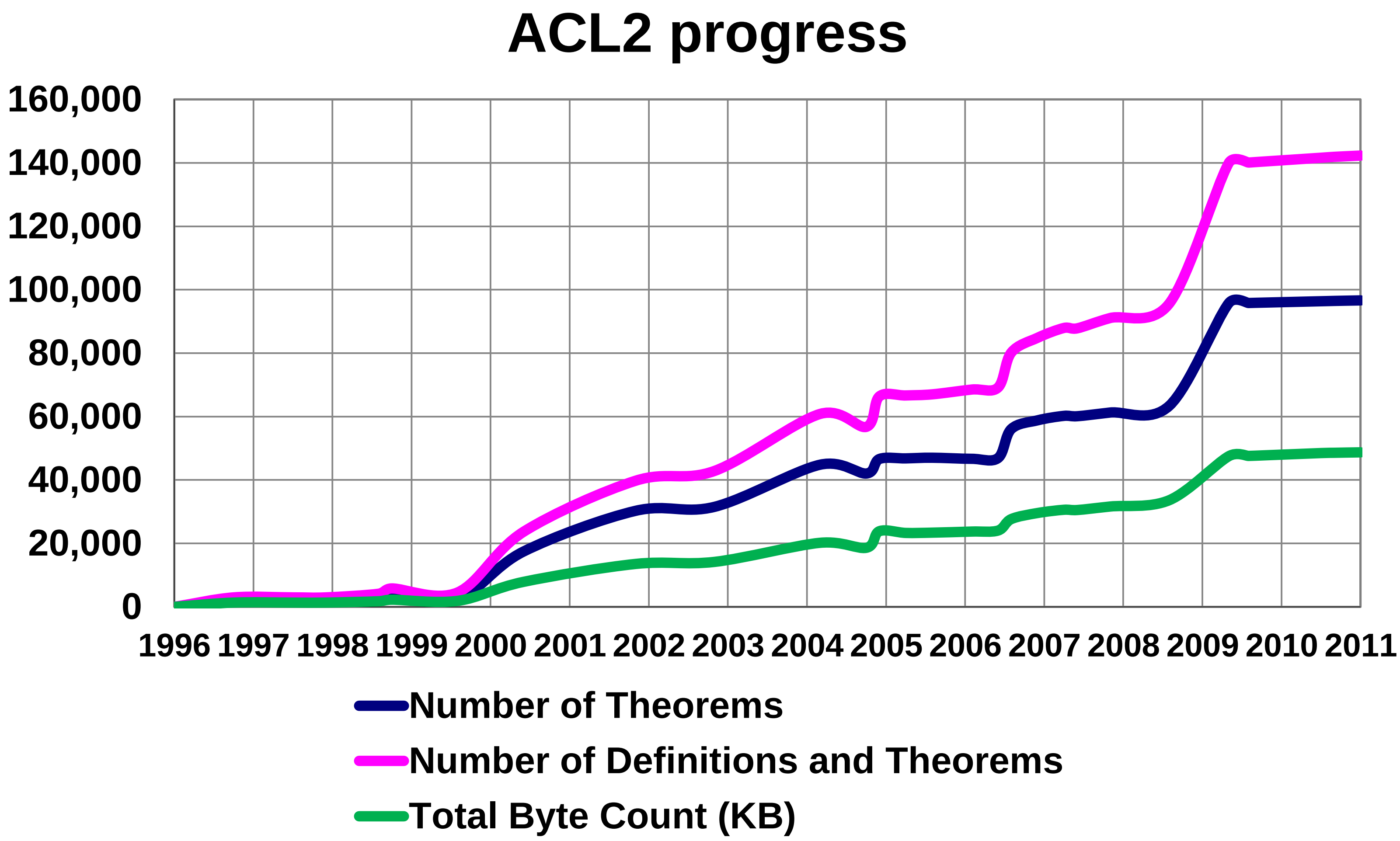


Progress: Model Checking



Numbers by Jason Baumgartner at IBM Austin

Progress: Theorem Proving



Numbers by J Moore, Matt Kaufmann, Warren Hunt, UT Austin

What is needed to bring these advances to bear on system security?

Tools that

- Generate assurance evidence as a system is built
- Can be easily understood and used by real programmers (and yield benefits they can see)
- Can support integration of evidence about various components
- Can be re-applied easily as systems evolve and adapt

Some Designed-In Security Research Challenges

- Mathematically sound techniques to support combination of models and composition of results from separate components
- Analysis techniques to enable traceable linking among diverse models and code
- Language design, processing, and tools that can provide high assurance for modular, flexible systems
- Team and supply chain practices to facilitate composition of assurance in the supply chain
- Tools to support assurance evidence management
- Learning what incentives (e.g. ability to quantify results) might motivate the use of these tools

Carl Landwehr

NSF

Federal Cybersecurity R&D Strategic Thrusts

- Research Themes
- ⇨Science of Cyber Security
- Transition to Practice
- Support for National Priorities

Science of Cyber Security

- A strategic research priority on the *science of security* to
  - Organize the knowledge in the field of security
  - Investigate universal concepts that are predictive and transcend specific systems, attacks, and defenses
  - Resulting in a cohesive understanding of underlying principles to enable investigations that impact large-scale systems
  - Enable development of hypotheses subject to experimental validation
  - Support high-risk explorations needed to establish such a scientific basis
  - Form public-private partnerships of government agencies, universities, and industry

Security Science

Today

- Mature **Crypto** Science
  - Adversary Models
  - Work Factor Metrics
  - Tempest, Physical Eng'g, etc.
- Formal Analysis Technology
  - Correctness Techniques/Tools
  - Protocol Verification
  - Efficient State Space Analysis
- Ad Hoc Cyber Engineering
  - Informal principles
  - Rudimentary Adversary Models
  - Process oriented Metrics
- Fragmented SoS Community

Future

- Mature **Cyber Security** Science
  - Formal Cyber Adversary Models
  - Cyber Security Metrics
  - Design & Implementation Support
- Objective Evaluation Techniques
  - Rigorous Toolset
  - Repeatable
- Trust Engineering Methodology
  - Construction/Composition Tools
  - Principled Design
  - Formal Discipline
- Coordinated SoS Community
  - Persistent, Self sustaining
  - Collaborative Structures (VO, Interest Grps)

Science of Cyber Security Questions

- What can we take from other sciences?
  - Are there any “laws of nature” in cyberspace that can form the basis of scientific inquiry in the field of cyber security?
  - Are there specific mathematical abstractions or theoretical constructs that should be considered?
  - Are there philosophical/methodological foundations of science that the cyber security research community should adopt?
- What sciences can we leverage?
  - Which scientific domains and methods, such as complexity theory, physics, theory of dynamical systems, network topology, formal methods, discrete mathematics, economics, social sciences, etc. can contribute to a science of cyber security?

Science of Cyber Security Questions (2)

- What is measurable in cyber security?
  - Currently security measures are very weak
  - How can we improve our ability to quantify cyber security?
- What is the role of experiments?
  - How do we structure efforts to do meaningful experiments?
- What theories can we expect?
  - How can we develop functional theories concerning complex computational processes?
  - How can we develop sound theories of the users and their interactions with the systems?
  - How can we develop sound theories of the adversary?

Science of Cyber Security Questions (3)

- How do we account for the human element in security?
  - Nature just exists, but adversaries cheat and use strategies to creatively violate models and assumptions
  - For any model of computer security, an adversary only needs to attack successfully one assumption of the model to subvert the security
- We need better models for analyzing how to achieve desired functions in systems with damaged and degraded or partial capabilities
  - Models of security tend to be binary (secure/unsecure) and localized within boundaries or abstraction layers
  - We need ways to reason about uncertainty and results within tolerances

Science of Cyber Security Questions (4)

- What are the impediments to advancing a scientific basis for cyber security?
- What measures and metrics can help us assess progress?
- Is there a special role for Government?

Some Potential Science of Security Research Topics

- Methods to model adversaries
- Techniques for component, policy, and system composition
- A control theory for maintaining security in the presence of partially successful attacks
- Sound methods for integrating the human in the system: usability and security
- Quantifiable, forward-looking, security metrics (using formal and stochastic modeling methods)
- Measurement methodologies and testbeds for security properties
- Development of comprehensive, open, and anonymized data repositories

Doug Maughan

DHS

Transition to Practice

- Concerted effort to get results of federally funded research into broad use
  - Integrated demos
  - Conferences and workshops
  - “Matchmaking” efforts
    - Among Agencies
    - Between research and product
  - Potential funding for last mile

Support for National Priorities

- Goals
  - Maximize cybersecurity R&D impact to support and enable advancements in national priorities
- Examples of Supported National Priorities
  - Health IT
  - Smart Grid
  - Financial Services
  - National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - National Initiative for Cybersecurity Education (NICE)

FY 2012 Budget Proposal / Cybersecurity R&D

- FY 2012 Budget Proposal / Cybersecurity R&D
  - Requested increase of 35% for cybersecurity research, development, and education ($407M FY10 to $548M FY12)
- Highlights
  - New NSF programs in the science of cybersecurity and game-changing research
  - Increased DOE investment in industrial control-system cybersecurity
  - New DARPA initiatives in information assurance, survivability, security by design, and insider threat mitigation
  - New NIST support for the National Initiative for Cybersecurity Education (NICE) and for the National Strategy for Trusted Identifies in Cyberspace (NSTIC)
  - Increase of 51% in cybersecurity R&D budget at DHS S&T

Summary

- Coordinated effort among government agencies
- Focus on game-changing themes
  - Encourages research collaborations based on tangible topics and desired future capabilities
- Strategic Plan for Federal Cybersecurity R&D Program
  - To be released soon, followed by a public comment period

For More Information

Tomas Vagoun, PhD
CSIA IWG Technical Coordinator

National Coordination Office for
Networking and Information Technology Research and Development
Suite II-405, 4201 Wilson Blvd.
Arlington, VA 22230
Tel: (703) 292-4873
vagoun@nitrd.gov

http://www.nitrd.gov
http://cybersecurity.nitrd.gov